(12) UK Patent Application (19) GB (11) 2 361 156 (13) A

(43) Date of A Publication 10.10.2001

(21) Application No 0008673.6

(22) Date of Filing 07.04.2000

(51) INT CL[7]
H04Q 3/00 // H04L 12/24 12/56

(52) UK CL (Edition S)
H4P PEUX

(56) Documents Cited
WO 00/03550 A1 US 5742762 A

(58) Field of Search
UK CL (Edition R) H4K KFM KF42 , H4P PEUL PEUM PEUX PPBC
INT CL[7] H04L 12/24 12/26 12/56 , H04Q 3/00
Online Databases: WPI, EPODOC, JAPIO

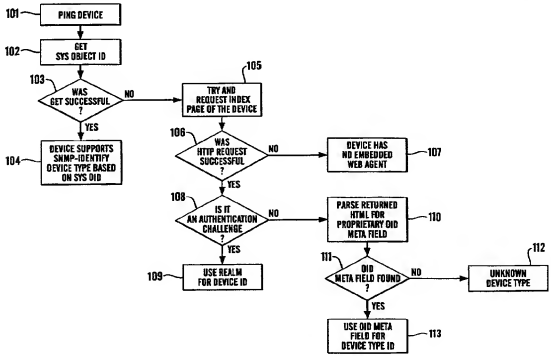
(71) Applicant(s)
3Com Corporation
(Incorporated in USA - Delaware)
5400 Bayfront Plaza, M/S 1308, Santa Clara,
California 95052-8145, United States of America

(72) Inventor(s)
Brendan Boulter
Christopher Robert Linzell
Simon Peter Valentine

(74) Agent and/or Address for Service
Brookes Batchellor
102-108 Clerkenwell Road, LONDON, EC1M 5SA,
United Kingdom

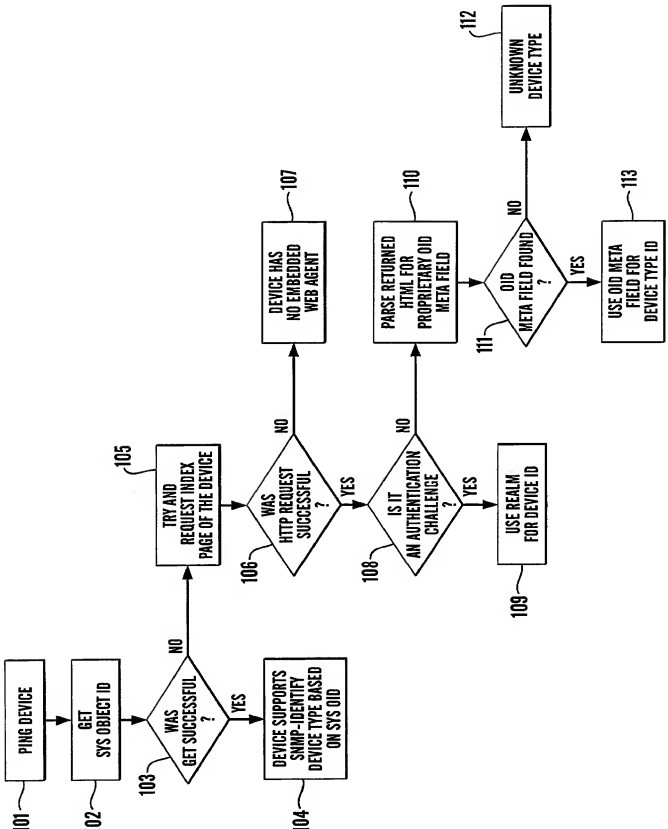
(54) Abstract Title
Discovering non-managed network devices using HTTP

(57) Network devices which are not SNMP enabled can be discovered using HTTP requests. When the network supervisor's computer interrogates the HTTP enabled device it makes an HTTP request for a device resource and receives back the response and in addition device identification information. This information can be extracted by analysing the 'realm' field of the authentication challenge. Where the device is not protected by an HTTP authentication mechanism the device type information is supplied by embedding this information in the <HEAD> section of the requested HTML document using a HTML <META> tag.



GB 2 361 156 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.


PING DEVICE
101
GET SYS OBJECT ID
102
WAS GET SUCCESSFUL ?
103
NO
YES
DEVICE SUPPORTS SNMP-IDENTIFY DEVICE TYPE BASED ON SYS OID
104
TRY AND REQUEST INDEX PAGE OF THE DEVICE
105
WAS HTTP REQUEST SUCCESSFUL ?
106
NO
YES
DEVICE HAS NO EMBEDDED WEB AGENT
107
IS IT AN AUTHENTICATION CHALLENGE ?
108
NO
YES
USE REALM FOR DEVICE ID
109
PARSE RETURNED HTML FOR PROPRIETARY OID META FIELD
110
OID META FIELD FOUND ?
111
NO
YES
UNKNOWN DEVICE TYPE
112
USE OID META FIELD FOR DEVICE TYPE ID
113

DISCOVERING NON MANAGED DEVICES IN A NETWORK SUCH AS A LAN USING HTTP

BACKGROUND OF THE INVENTION

The present invention relates to a method and apparatus for discovering non managed devices (e.g. devices that do not have an SNMP (Simple Network Management Protocol) agent) in a network such as a LAN (Local Area Network) or other network. The preferred embodiment of the present invention relates to the discovery of devices that do not have an SNMP agent but do include an embedded web agent.

The present invention relates to the process of discovery of the devices on network, that is a network of electronic devices comprising, for example, workstations, personal computers, servers, hubs, routers, bridges, switches, (hereinafter referred to as devices of the network), and links between these devices which may be in the form of physical cable or wireless links. The network may be a local area network (LAN), such as an Ethernet network, wide area network (WAN) or other types, including wireless networks.

Computers and other devices connected to a network may be managed or unmanaged devices. A managed device has processing capability, which enables it to monitor data traffic sent from, received at, and passing through the ports of the device. Monitored data associated with the ports of the network device is stored in memory on the network device. For example, data relating to the origin of a data packet which is received at a port is stored along with the identity of the relevant port.

After such a network has been installed, it is desirable for the person appointed network manager to be able to understand the technical operation of the network. In known network management systems, the manner in which the relevant data is retrieved from the managed devices, compiled and displayed "discovered" has been problematic in several respects. Primarily the data does not provide information about

unmanaged (eg non SNMP enabled) devices.

The topology of the network may be deduced by the network manager's computer by the process of discovery in which each of the devices of the network is interrogated to thereby produce on a network manager's workstation details of the network and its operation, preferably in the form of a network map which may be displayed on a visual display unit showing the devices and links between the devices. At its simplest, and where the device is a "managed" device, this information is usually provided by interrogation using a known protocol, such as the SNMP (Simple Network Management Protocol), of the so-called 'agent' of each device which stores the device's unique MAC address, the type of device and the MAC addresses embedded in the data passing into a particular port which thereby gives the MAC addresses of the origin of the data and hence the MAC address of the devices which are connected to the ports directly or indirectly.

Many devices are not SNMP enabled and so the discovery or interrogation of the network produces a result which indicates that these non SNMP enabled devices are displayed as "generic" devices.

It would be desirable if one were able to deduce more information about these generic devices, that is non-SNMP enabled devices, and the present invention provides a method of doing so.

SUMMARY OF THE INVENTION

The present invention provides a device for use in a network, said device including information identifying the device, which information is made accessible during HTTP (Hyper Text Transfer Protocol) authentication procedure.

In one arrangement, where the device implements a security mechanism, the device includes means whereby the identifying information is transmitted in response to a challenge request.

In an alternative arrangement, in which the device does not implement a security mechanism, the information identifying the device is added to the head section of an HTML document provided in response to a request by the user.

BRIEF DESCRIPTION OF THE DRAWING

A preferred embodiment of the invention will now be described by way of example only and with reference to the accompanying drawing which is a flow chart of a method of discovery of devices, which method includes steps for discovering HTTP enabled but not SNMP enabled devices on a network, which HTTP enabled devices may or may not include a security mechanism.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The physical network to be discovered may comprise a plurality of devices in the form of a network supervisor's workstation or computer, other workstations, hubs, or switches.

The devices are connected together by means of links which may be hard wired or wireless and utilise any desired protocol.

The network supervisor's workstation includes, in addition to a visual display unit, a central processing unit or signal processor, a selector which may be in the form of a mouse, a program store which may comprise, for example, a CD drive, a floppy disk drive or a zip drive, and a memory for storing a program which may have been loaded from the program store or downloaded for example via Internet from a website.

To discover the network, using SNMP, the network supervisor's computer interrogates each device and analyse the network, and stores in the memory the information relating to the devices within the network and the links between the devices. In essence, managed devices include a so-called agent which in the case of an SNMP agent stores information about the device such as its unique MACaddress, its Sys Object ID (which identifies what the device is and its model type), how many ports it has, and the MAC address of the origin of the data which at least some of the ports have received and hence to which they are directly or indirectly connected. The computer interrogates the agents of each device.

In a preferred arrangement, the computer may, on command from the selector, process signals from the memory by the signal processor and provide on the visual display unit a network map showing each of the devices and the links therebetween. In the examples described, the network is simple but of course in many instances the network will be considerably more complex and it may be necessary to arrange that the visual display unit only shows a simplified version or only part of the network at any one time.

As mentioned above, however, whilst many devices may support (ie communicate using) the SNMP protocol and hence will be discovered and represented by the relevant icon in its correct location on the network map, some devices do not support the SNMP protocol. Examples of such devices are simple switches, network appliances such as firewalls and web caches and indeed work stations. Thus discovering the network using SNMP (or indeed any other related protocol) will mean that these devices will appear as icons representing unmanaged generic devices, in other words, the SNMP protocol will not allow for proper discovery of the identity of these devices. The inventors of this invention have invented an alternative method of identifying these non-SNMP enabled devices and providing relevant details by using a different protocol, ie not SNMP.

Some or all of the devices which are not SNMP enabled will be HTTP enabled.

As is known, a device which is HTTP enabled (which includes many devices including, for example, network device such as a firewall) receives HTTP requests on its TCP port 80. The device may or may not include a security mechanism and we will describe alternative arrangements covering the two cases.

DEVICES WITH SECURITY MECHANISM
HTTP AUTHENTICATION MECHANISM

Firstly, it will be assumed that the device includes a security mechanism in which the device will only allow access to a client if the client is authorised. Thus the device's files and resources are protected by the standard HTTP authentication mechanism. When a web client (for example, a browser) requests a document or resource from an HTTP enabled device, the device requires the web client to authenticate itself so as to establish that the client is authorised to access the document or resource. The device using HTTP identifies the authentication of realm which applies to the requested resource and also the authentication mechanism.

For example, the web client requests information from the HTTP device by passing a request to the device as follows:

```
GET /
HTTP/1.0 ..... (1)
```

(i.e. the web client has requested information and has set out the protocol required.)

The device may respond to this where there is security by returning the following message:

```
HTTP/1.0 401 unauthorised .....(2)
WWW-Authenticate: Basic realm="device" .....(3)
```

The device will then normally pass to the web client a dialog box requesting a valid user name and password for the requested resource in the named security realm (in this case "device"). The web client then re-requests the resource from the device, using an authorisation field which identifies the authentication mechanism and the encoded or encrypted user response:

```
GET /
HTTP/1.0
Authorisation: basic YwrTaW46
```

When the string "YwrTaW46" is decoded by the device using the "Basic" authentication mechanism, it yields the username and password. If valid, the requested resource is then returned to the web client.

In the present arrangement the HTTP authentication mechanism is extended by adding device identification information to the challenge request. When the network supervisor's computer (acting like the "web client" above) interrogates the HTTP enabled device, it makes an HTTP request (line (1) above) for a device resource and receives back the response (lines (2) and (3) above) and in addition device identification information. For example device response is changed as follows:

```
HTTP/1.0 401 unauthorised .....(2)
WWW-Authenticate:Basic realm="1.2.3.4.5.6" .....(3A)
```

(Where the identity of the device is "1.2.3.4.5.6")

The computer can then extract the device identification information by analysing the "realm" field of the authentication challenge. Thus in this new arrangement, the computer simply makes a HTTP request for a device resource and then extracts the device type information by analysing the "realm" field of the authentication challenge.

The device type information can be defined either statically (during the software development for the device) or dynamically upon receipt of a HTTP request by the device.

DEVICE WITHOUT SECURITY MECHANISM

In alternative arrangements where device security is not provided the arrangement is as follows.

Thus where the device's files and resources are not protected by an HTTP authentication mechanism, the device type information is supplied by embedding this information in the document's <HEAD> section using a HTMP <META> tag.

The <HEAD> section of a HTML document is intended to supply information about the document. Within the <HEAD> section, it is proposed to use the HTML 4.0 standard <META> tag to supply the device type information. The <META> tag is used to declare a document property (eg author, title, keyword) and a value associated with that property. In this arrangement, a document property called "sysObjectID" is defined in the <HEAD> section and the value of the device type is assigned to it.

Typically, Web servers are configured to return a predetermined page if no page has been explicitly requested by the user. This is called the "index" page. The present arrangement embeds the device type information in the <HEAD> section of the index page as follows:

```
<HTML>
<HEAD>
<META NAME ="sysObjectID" CONTENT="1.2.3.4.5.6">
---
---
```

</HEAD>
<BODY>

</BODY>
</HTML>

Having deduced the identification information of the device, the network manager's computer is then able to produce a network map on which the device is identified with the relevant information. For example, that information may set out what the device is (work station, printer, etc), what model of device it is (that is the manufacturer and model number), the configuration of the device, the status of the device and such other information as may be useful.

The preferred method of the invention is carried out under the control of the network manager's workstation or computer and in particular by means of a program controlling the processor apparatus of that computer or elsewhere in the system.

The program for controlling the operation of the invention may be provided on a computer readable medium, such as a CD, or a floppy disk, or a zip drive disk carrying the program or their equivalent, or may be provided on a computer or computer memory carrying the website of, for example, the supplier of the network products. The program may be downloaded from whichever appropriate source and used to control the processor to carry out the steps of the invention as described.

The program may include an algorithm of the form set out in the flow chart of the drawings.

Thus the program may include the following steps:

program step 101, to cause the network manager's computer to ping a device;

program step 102, to receive sysObjectID from pinged device;

program step 103, was obtaining sysObjectID successful?

if obtaining sysObjectID was successful, (i.e. thedevice supports SNMP), at program program step 104, identify the device type based on sysObjectID and display device type on network map;

if obtaining sysObjectID was unsuccessful, at program step 105, request index page of the device using HTTP;

at program step 106, was HTTP request successful?

if HTTP request was not successful (device has no embedded web agent) in step 107, display device as generic device on network map;

if HTTP request was successful, at program step 108 was it an authentication challenge?

if yes, at program step 109 use realm for device type identification and display relevant device type on network map;

if no, at program step 110, parse returned HTTP for proprietary OID meta field;

program step 111, was OID meta field found?;

if no, program step 112, display generic type device on network map;

if yes, at program step 113, use OID meta field to obtain device type ID and display relevant device on network map.

The invention is not restricted to the details of the foregoing example.

CLAIMS

1. A device for use in a network, said device including information relating to the device, including means whereby said information is made accessible during an HTTP authentication procedure.

2. A device as claimed in claim 1 wherein the device implements a security mechanism, the device including means whereby the information is transmitted in response to a challenge request.

3. A device as claimed in claim 2 in which the information is included in the realm field of the authentication challenge.

4. A device as claimed in claim 1 wherein the device does not implement a security mechanism, and the information is included in the head section of an HTML document provided in response to a request.

5. A device as claimed in any of claims 1 to 4 in which the relevant information is identifying information identifying the device.

6. A device as claimed in any of claims 1 to 5 in which the relevant information is information relating to the configuration of the device.

7. A device as claimed in any of claims 1 to 6 in which the relevant information is information relating to the status of the device.

8. A method for obtaining information regarding a device in a network, said method including obtaining said information during an HTTP authentication procedure.

9. A method as claimed in claim 8 wherein the device implements a security mechanism, and the information is transmitted in response to a challenge request.

10. A method as claimed in claim 9 in which the information is included in the realm field of the authentication challenge.

11. A method as claimed in claim 8 wherein the device does not implement a security mechanism, and the information is included in the head section of an HTML document provided in response to a request.

12. A method as claimed in any of claims 8 to 11 including using said information to provide a relevant icon on a network map.

13. A method as claimed in any of claims 8 to 12 in which the relevant information is identifying information identifying the device.

14. A method as claimed in any of claims 8 to 13 in which the relevant information is information relating to the configuration of the device.

15. A method as claimed in any of claims 8 to 14 in which the relevant information is information relating to the status of the device.

16. A computer program on a computer readable medium loadable into a digital computer or embodied in a carrier wave, said program including software for carrying out the method of any of any of claims 8 to 15.

Application No: GB 0008673.6 **Examiner:** Gareth Griffiths
Claims searched: All **Date of search:** 3 October 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): H4K (KFM, KF42), H4P (PEUL, PEUM, PEUX, PPBC)

Int Cl (Ed.7): H04L 12/24, 12/26, 12/56, H04Q 3/00

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	WO00/03550 A1	(ERICSSON) p.6 line 13 - p.7 line 7	1, 5-8, 12-15
A	US5742762	(SCHOLL) whole document	

X Document indicating lack of novelty or inventive step
Y Document indicating lack of inventive step if combined with one or more other documents of same category.
& Member of the same patent family

A Document indicating technological background and/or state of the art.
P Document published on or after the declared priority date but before the filing date of this invention.
E Patent document published on or after, but with priority date earlier than, the filing date of this application.